

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PRE-APPEAL BRIEF REQUEST FOR REVIEW</b>		Docket Number (Optional) 3037-4196	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]		Application Number 09/630,711	Filed August 1, 2000
		First Named Inventor Bjorn Markus JAKOBSSON	
on _____	Art Unit 2131	Examiner Aravind K. Moorthy	
Signature _____	Confirmation No. 7518		
_____ Type or printed name			

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).  
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor. \_\_\_\_\_  
Signature

☐ assignee of record of the entire interest.  
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96) \_\_\_\_\_  
Joseph C. Redmond, Jr.  
Type or printed name

☒ attorney or agent of record.  
Registration number 18,753 \_\_\_\_\_  
202-857-8010  
Telephone number

☐ attorney or agent acting under 37 CFR 1.34.  
Registration number if acting under 37 CFR 1.34 \_\_\_\_\_  
August 23, 2007  
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

<input type="checkbox"/> *Total of _____ forms are submitted.
---

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Serial No.:	09/630,711	Confirmation No.:	7518
Applicants:	Bjorn Markus JAKOBSSON <i>et al.</i>	Group Art Unit:	2131
		Examiner:	Aravind K. Moorthy
Filed:	August 1, 2000		
		Customer No.:	27123
For:	PROOFS OF WORK AND BREAD PUDDING PROTOCOLS		

**NOTICE OF APPEAL & PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Mail Stop **AF**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

In response to the Advisory Action dated June 4, 2007, Applicants submit herewith a Notice of Appeal for the subject application and an accompanying Pre-Appeal Brief Request for Review pursuant to the USPTO OG Notices: February 7, 2006, as follows:

**I. Claims Under Appeal:**

24. (Previously Presented) A method of using a computational effort invested in a proof of work (POW), the method executable in one or more processors in communication with one or more memory devices having embodied therein stored programs for performing the method, comprising:

generating a computational task for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation;

distributing the computational task for execution among a plurality of server entities receiving a POW relating to said task from one of said plurality of said server entities; using said POW to verify and accomplish said computational task; and distribution of the POW as a POW.

31. (Previously Presented) A method of using a computational effort invested in a proof of work (POW), the method executable in one or more processors in communication with one

or more memory devices having embodied therein stored programs for performing the method, comprising:

generating a computational task by a first server for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation;

distributing the computational task by the first server for execution among a plurality of second servers;

receiving at the first server a POW relating to said task from one of said plurality of said second servers;

using said POW by the first server to verify and accomplish said computational task; and

re-using of the POW as a POW in another task.

## **II. Status of Claims:**

Claims 1-31 are pending in the application, and comprise allowable subject matter.

Claim 31 is rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claims 24 and 31 stand rejected under 35 U.S.C. § 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

## **III. Review Request:**

Applicants request review by the Conference of Examiners of the final rejection of independent claims 24 and 31 under 35 U.S.C. § 112, first and second paragraph, and provides response to the rejections, as follows:

### **A. Claim 31:**

The Examiner contends that Claim 31 does not comply with the written description requirement based on there is no support in the specification for the feature “generating a computational task by a first server for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation;”

Applicants direct the Conference of Examiners attention to the specification at page 3, line 13, continuing to page 4, line 2, where it is stated:

“As shown in FIGS. 1A and 1B, the architecture comprises entities 1, 2 and 3 through n (all of which may be servers). Although entity 1 is illustrated in FIGS. 1A and 1B as being distinct

from entity 2, in an alternate embodiment, entities 1 and 2 may be the same entity. To begin, with reference to FIG. 1A, entity 1 has a computational task to perform. In furtherance of that task, (A) entity 1 instructs entity 2 to perform some computational work related to the task. Entity 2 will then out-source the work related to the task to each of entities 3 through n. Outsourcing may be accomplished by dividing the work into components and assigning each entity 3 through n a different component. As shown in FIG. 1B, as (B) each entity 3 through n completes its component of work, each entity will respond with its reply. Each of the replies is a POW (referred to herein as "POW<sub>i</sub>"). Entity 2 then complies (compiles) the replies into a response and transmits the response to entity 1. This response is also a POW (referred to herein as "POW<sub>2</sub>"). Finally, (C) entity 1 verifies the response."

Applicants submit the terms "generating a computational task by a first server" are described by the underlined portion of the specification, identified above as (A).

Applicants further submit the terms "for a certain amount of intense computation in a specified period of time as a POW" are described by the underlined portion of the specification, identified above as (B).

Applicants further submit the terms "to accomplish a separate, useful and verifiable correct computation" are identified by the underlined portion of the specification, identified above as (C), taken in conjunction the underlined portion of the specification at page 2, lines 14-17, where it is stated, "Whereas the traditional bread pudding recipe recycles stale bread, a bread pudding protocol recycles the "stale" computations in a POW to perform a separate and useful operation, while also maintaining privacy in the operation."

Applicants submit that a worker skilled in the art, particularly the computational art, has sufficient disclosure from the above cited specification pages to implement the claimed feature.

The rejection of claim 31 under 35 U.S.C. § 112, first paragraph, is believed overcome by the indicated disclosures in the specification. Withdrawal of the rejection of claim 31 under 35 U.S.C. § 112, first paragraph, is requested.

**B. Claims 24 and 31:**

The Examiner contends that "claims 24 and 31 recite the limitation 'generating a computational task by a first server for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate, useful and verifiable correct computation.' The Examiner asserts that the phrases 'certain amount', 'intense' and 'useful' are indefinite terms."

Applicants reply, as follows:

1. With regard to the phrases “certain amount” and “intense”, Applicants direct the Conference of Examiners’ attention to the specification at page 5, line 12, continuing to page 6, line 4, which states, as follows:

“The aim of a POW is to enable P to demonstrate that she has performed a certain amount of computation within the time interval  $[-t_s, t_c]$ . Let poly denote any polynomial in a given variable. (We use the informal notation poly(x) to denote a polynomial in the variable x, and  $o(1/\text{poly}(x))$  to denote a quantity that is asymptotically smaller than the inverse of any polynomial in x.) Finally, let l be a security parameter. Finally, let us assume that the prover is permitted to perform an arbitrarily large amount of computation prior to the protocol execution. Thus, in fact, our definitions assume that the prover may perform computation over the time interval  $[-\infty, t_c]$ . We characterize the hardness of a POW using the following two definitions, where probabilities are over the coin flips of both parties, and computational steps and memory resources are as measured in any suitable model. Definition 1 provides the notion of a lower bound on POW hardness, while Definition 2 provides that of an upper bound.

Definition 1: We say that a proof of work POW is (w, p)-hard if the following is true. Suppose prover P with memory resources bounded by m performs an average, over all coin flips by P and V, of at most w steps of computation in the time interval  $[t_s, t_c]$ . Then the verifier V accepts with probability at most  $p + o\left(\frac{m}{\text{poly}(l)}\right)$ , where l is a security parameter.

Definition 2: We say that a proof of work POW is (w, p, m)-feasible if there exists a prover P with memory resources bounded by m such that with an average of w steps of computation in the time interval  $[t_s, t_c]$ , the prover can cause the verifier V to accept with probability at least p. This leads to the following definition.

Applicants submit the Definitions 1 and 2 define the phrases “certain amount” and “intense” by the number of flips of at most w steps of computation in the time interval  $t_s, t_c$  for a verifier to accept a POW with at least a probability p.

A worker skilled in the art, particularly one skilled in the computational art, has sufficient information from the cited specification pages to implement the claimed feature in which the phrases “certain amount” and “intense” are used.

2. With regard to the phrase “useful”, applicants direct the Conference of Examiners’ attention to the specification at page 1, line 13-16 which states, as follows:

Pre-Appeal Brief Request for Review Response to 06/04/2007, Advisory Action

“Although not defined as such or treated formally in the literature, POWs have served as the basis for a number of data security applications, including, benchmarking, server access metering, construction of digital time capsules, and protection against spamming and other denial-of-service attacks.”

Applicants submit the above specification portion describes separate and useful applications of POWs. A worker skilled in the art, particularly the computational arts would recognize the usefulness of the claimed subject matter.

**C. Affidavit under 37 CFR 1.132**

Applicants attach as Exhibit A an Affidavit under 37 CFR 1.132 by Dr. Ganapathy S. Sundaram declaring that one skilled in the art would be able to implement and use the claimed subject matter using the disclosure as a guide, based on the technical subject matter described in the specification.

**CONCLUSION:**

Applicants have demonstrated support in the specification for the terms and phrases in the claimed subject matter. The rejection of claim 31 under 35 U.S.C. § 112, first paragraph, and the rejection of claims 24 and 31 under 35 U.S.C. § 112, second paragraph, have been overcome. Claims 1-31 have been deemed allowable subject matter. Having overcome the rejections of claims 24 and 31, Applicants request allowance of claims 1-31, and passage to issue of the case.

Respectfully submitted,  
MORGAN & FINNEGAN, L.L.P.

Dated: August 23, 2007

By:

Joseph C. Redmond, Jr.

Correspondence Address:

Registration No. 18,753

Address Associated With Customer Number:

27123

(202) 857-7887 Telephone

(202) 857-7929 Facsimile